Background

Read-only Domain Controllers are sometimes configured to allow password caching.
They are sometimes also managed by non-admin users, that might be easy to compromise.
If you manage to compromise the RODC administrator you can dump the cached credentials from the RODC.

How to check for

How to exploit

Recommendation

References

https://adsecurity.org/?p=3592